APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/663,478	09/15/2003	James R. Trethewey	42P17784	2896

59796   7590   02/03/2011
INTEL CORPORATION
c/o CPA Global
P.O. BOX 52050
MINNEAPOLIS, MN 55402

EXAMINER
TRUVAN, LEYNNA THANH

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
02/03/2011	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

heather.l.adamson@intel.com

	Application No.	Applicant(s)
Office Action Summary	10/663,478	TRETHEWEY ET AL.
	Examiner	Art Unit	
	Leynna T. Truvan	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>19 November 2010</u>.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-3,5-13,15-25 and 27-33</u> is/are pending in the application.

    4a) Of the above claim(s) <u>4, 14, and 26</u> is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-3,5-13,15-25 and 27-33</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application

6)☐ Other: _____.

DETAILED ACTION

1.   Claims 1-3, 5-13, 15-25, and 27-33 are pending.

        Claims 4, 14, and 26 have been cancelled by applicant.

2.   Claims 1-3, 5-7, and 29 was previously rejected under 35 U.S.C. 101, are now

withdrawn due to the current amendment.

Response to Arguments

3.   Applicant's arguments filed 11/19/10 have been fully considered but they are not

persuasive.

        <u>Regarding the argument on p.8</u>, that Moles teaches one location privacy flag that

is either set to not transmit the location or not set to transmit location which does not

teach or suggest the claimed "requesting the privacy preferences associated with each

of the plurality of location properties the requestor from the user, wherein the privacy

preference location information is to be shared with and/or blocked from the requestor".

As mentioned in the last office action, claim 1 recites the limitation "<u>if</u> privacy

preferences associated with the requestor have not been specified", where the term "if"

broadly suggests that in the event that something does not or has not occurred, which in

this case the claimed request has not been specified, then to go to the next specified

step. So when (and/or if) privacy preferences associated with the request have been

specified, then the claimed "if...not been specified" is not effective and privacy

preferences from each of the plurality of locations are not needed from the user. And

also can broadly mean that the privacy preferences associated with the plurality of location properties are not necessarily needed or requested if the privacy preferences associated with the requestor have been specified. In the event if the privacy preferences have not been specified, then the claimed privacy preferences associated with each of the plurality of location properties are requested from the user. As for Moles, discloses the privacy flag record records the time and date of each occurrence of location privacy flag being enabled or disabled (col.9, lines 50-60). By Moles citing there's recording of each occurrence of location privacy flag obviously suggests there are multiple or plurality of privacy preferences associated with plurality of location properties. Moles also discusses setting and testing separate additional location privacy status flags for data and voice calls in the memory unit (col.11, lines 15-18). The additional location privacy status flags obviously suggest there is privacy preferences associated with each of the plurality of location properties. Therefore, Moles reads on the claimed invention.

Regarding argument on pg.9, examiner traverses the argument stating the Moles and Hertz combination does not solve the deficiencies of Moles for the reasons explained above. Examiner also traverses the argument that unlike the present invention, Moles requires the user to access the transmission status menu to answer the question of whether location information is to be transmitted because the claimed invention states the computing device requesting the privacy preferences. It's not as if the claim calls for the requestor requesting the location straight to the user nor is the request in real time to a user mobile. This is a distinction from what the current

limitation which claims the requestor requesting to a computing device and in turn the computing device makes the request to the user. As applicant pointed out, on col.6, line 60-col.7, line 3, the display unit which obviously is part of a computing device asks whether location information is to be transmitted and the user can selectively enable or disable the location privacy flag. Moles send a signal to each individual wireless mobile station which obviously can be a user to ask each GPS unit to transmit to the operator the exact location of the wireless mobile station in the which the GPS unit is located (col.2, lines 13-15). Hence, Moles reads on the claimed the computer device, requesting the privacy preference associated with each of the plurality of location properties the requestor from the user.

Regarding the argument on pg.10-12, that Hertz does not teach or suggests "if a privacy preference associated with the requestor has not been specified, requesting a privacy preference associated with the requestor from the user". Hertz includes the ability of queries and tasks requirements in the form of request (col.15, lines 4-6). Access control criteria dictating profile access and reach ability of the user and construction of conveniently navigable hierarchical menus (col.14, lines 15-17 and col.15, lines 12-25). Hertz also discloses data mining tools can be used to enable advertisers to identify relevant features and may enter rules that specify how users are to be targeted based on desired criteria (col.16, lines 1-7). Hertz suggests querying and database matching obviously suggests ability for determining if a privacy preference associated with the requestor has been specified or not and to enable or restrict the ability of an explicitly identified user (col.15, lines 16-20). With Hertz suggesting

querying with data mining tools and Moles capable of entering a response in response

to a question whether location information is to be transmitted. Therefore, Hertz

suggests the ability to request a privacy preference associated with the requestor from

the user in response to receiving the request if the privacy preference associated with

the requestor has not been specified.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

4.   **Claims 1-3, 5-13, 15-25, and 27-33 are rejected under 35 U.S.C. 103(a) as**

being unpatentable over Moles, et al. (US 6,505,048) in view of Hertz, et al. (US

6,571,279).

As per claim 1:

Moles disclose a <u>computer-implemented</u> method comprising:

receiving<u>, by a computer device,</u> a location request from a requestor for a

location associated with <u>the</u> computer device **(col.2, lines 10-15 and col.6, lines 21-25)**,

the location including a plurality of location properties; and **(col.6, lines 10-20 and col.7,**

lines 10-13)

if privacy preference associated with the requestor have not been specified

(col.2, line 60-col.3, line 2), <u>the computer device,</u> requesting **(col.6, line 20-col.7, line 3)**,

the privacy preference associated with each of the plurality of location properties (**col.9, lines 50-60 and col.11, lines 15-18**) the requestor from the user, wherein the privacy preference location information is to be shared with and/or blocked from the requestor. (**col.6, line 56 – col.7, line 28 and col.8, lines 37-64**)

The computer device can broadly be given as a wireless mobile station (col.4, lines 45-54). Moles teach the operator or (authorized) party requesting or receiving the mobile station's location reads on the requestor for the location of the computer device (col.2, lines 20-22 and 38-40). Moles discloses the user have the ability to selectively transmit the location of the wireless mobile station to authorized parties (col.2, lines 38-40). Moles also disclose a method fro selectively disabling the transmission of information concerning the location of the wireless mobile station (col.3, lines 40-44). This obviously suggests the ability to set to transmit or not transmit the location property to a particular requestor(s) which in Moles' instance, is for authorized parties (col.8, lines 37-64). Thus, Moles suggests the claimed determining whether a privacy preference associated with the requestor has been specified.

The claimed location properties can broadly be interpreted as data or information relating to the location which as claimed is associated to the computing device. Hence, the location properties can be reasonably be given as geographic location in terms of latitude and longitude of the mobile station (col.6, lines 10-20 and col.7, lines 10-13). Moles discusses the claimed privacy preference as the privacy flag where a value that has been set determines whether information of the location of the mobile station is to be transmitted (col.2, line 60 – col.3, line 2 and col.6, lines 56-61).

In addition, Moles discloses the privacy flag can selectively set to cause wireless the mobile station to not transmit location information of the mobile station and can set a value of location privacy flag whether location information is to be transmitted (col.6, line 56-col.7, line 5). Thus, obviously suggested sending location information if the privacy preference associated with the requestor has not been specified otherwise. However, Moles did not clearly explain the claimed requesting a privacy preference associated with the requestor if a privacy preference associated with the requestor has not been specified.

Hertz, et al. teaches the location enhanced information delivery system can improve the user-user automatic matching techniques by notifying users of other users that are located in or near the same vicinity and match the profile conditions as consistent with the privacy policies of users (col.13, lines 30-42). Hertz discloses access control criteria dictating profile access and reach ability of the user may be controlled accordingly based upon the profile of the requestor and/or the nature of the request (col.15, lines 11-36). Hertz includes the ability of queries and tasks requirements in the form of request (col.15, lines 4-6). Access control criteria dictating profile access and reach ability of the user and construction of conveniently navigable hierarchical menus (col.14, lines 15-17 and col.15, lines 12-25). Hertz also discloses data mining tools can be used to enable advertisers to identify relevant features and may enter rules that specify how users are to be targeted based on desired criteria (col.16, lines 1-7). Hertz suggests querying and database matching obviously suggests ability for determining if a privacy preference associated with the requestor has been

specified or not and to enable or restrict the ability of an explicitly identified user (col.15,
lines 16-20). With Hertz suggesting querying with data mining tools and Moles capable
of entering a response in response to a question whether location information is to be
transmitted. Thus, suggests the ability to request a privacy preference associated with
the requestor from the user in response to receiving the request if the privacy
preference associated with the requestor has not been specified.

Therefore, it would have been obvious for a person of ordinary skills in the art to
combine the teaching of Moles with Hertz to teach if a privacy preference associated
with the requestor has not been specified, requesting a privacy preference in response
to receiving the request because access control dictating profile access and reach
ability of the user may be controlled based upon the profile of the requestor such access
control may be used to enable/restrict access (Hertz-col.15, lines 11-46 and col.16,
lines 1-7).

As per claim 2: See Moles on col.2, lines 36-39 and col.2, line 66 – col.3, line 2;
discussing if a privacy preference associated with the requestor has been specified,
applying the specified preference to determine whether to provide the location to the
requestor.

As per claim 3: See Moles on col.2, lines 24-26 and 61-63 and col.7, lines 14-18;
discussing preventing the location from being provided to the requestor if the privacy
preference specifies that the location is to be kept private, and providing the location to
the requestor if the privacy preference specifies that the location is to be disclosed to
the requestor.

As per claim 14: Cancelled

As per claim 5: See Moles on col.6, lines 21-24 and Hertz on col.18, lines 52-55;

discussing requesting includes providing a pop-up dialog box.

As per claim 6: See Moles on col.6, lines 57-65; discussing providing a pop-up dialog

box includes enabling a user to selectively enable and disable privacy for individual

location properties.

As per claim 7:

Moles disclose a computer-implemented method comprising:

      enabling, by a computer device, a user to selectively enable and disable location-

aware computing on the computer device; and **(col.2, lines 34-48)**

      preventing a location of the computer device, from being provided to a requestor

if the user has disabled location-aware computing; **(col.2, lines 24-26 and 61-63 and**

col.7, lines 14-18)

      if the user has enabled location-aware computing and **(col.7, lines 5-12 and**

col.10, lines 37-57) *if* privacy preferences associated with each of the plurality of location

properties **(col.6, lines 10-20 and col.7, lines 10-13)** for the requestor have not been

specified **(col.2, line 60-col.3, line 2 col.9, lines 50-53)**, requesting **(col.6, line 20-col.7, line**

3) the privacy preference associated with each of the plurality of location properties

(col.9, lines 50-60 and col.11, lines 15-18) for the requestor from the user for a location

associated with a computing device, wherein the privacy preference indicates location

information to be shared with and/or blocked from the requestor. **(col.6, line 56 – col.7,**

line 28 and col.8, lines 37-64)

The computer device can broadly be given as a wireless mobile station (col.4, lines 45-54). Moles teach the operator or (authorized) party requesting or receiving the mobile station's location reads on the requestor for the location of the computer device (col.2, lines 20-22 and 38-40). Moles discloses the user have the ability to selectively transmit the location of the wireless mobile station to authorized parties (col.2, lines 38-40). Moles also disclose a method fro selectively disabling the transmission of information concerning the location of the wireless mobile station (col.3, lines 40-44). This obviously suggests the ability to set to transmit or not transmit the location property to a particular requestor(s) which in Moles' instance, is for authorized parties (col.8, lines 37-64). Thus, Moles suggests the claimed determining whether a privacy preference associated with the requestor has been specified.

The claimed location properties can broadly be interpreted as data or information relating to the location which as claimed is associated to the computing device. Hence, the location properties can be reasonably be given as geographic location in terms of latitude and longitude of the mobile station (col.6, lines 10-20 and col.7, lines 10-13). Moles discusses the claimed privacy preference as the privacy flag where a value that has been set determines whether information of the location of the mobile station is to be transmitted (col.2, line 60 – col.3, line 2 and col.6, lines 56-61).

In addition, Moles discloses the privacy flag can selectively set to cause wireless the mobile station to not transmit location information of the mobile station and can set a value of location privacy flag whether location information is to be transmitted (col.6, line 56-col.7, line 5). Thus, obviously suggested sending location information if the privacy

preference associated with the requestor has not been specified otherwise. However, Moles did not clearly explain the claimed requesting a privacy preference associated with the requestor if a privacy preference associated with the requestor has not been specified.

Hertz, et al. teaches the location enhanced information delivery system can improve the user-user automatic matching techniques by notifying users of other users that are located in or near the same vicinity and match the profile conditions as consistent with the privacy policies of users (col.13, lines 30-42). Hertz discloses access control criteria dictating profile access and reach ability of the user may be controlled accordingly based upon the profile of the requestor and/or the nature of the request (col.15, lines 11-36). Hertz includes the ability of queries and tasks requirements in the form of request (col.15, lines 4-6). Access control criteria dictating profile access and reach ability of the user and construction of conveniently navigable hierarchical menus (col.14, lines 15-17 and col.15, lines 12-25). Hertz also discloses data mining tools can be used to enable advertisers to identify relevant features and may enter rules that specify how users are to be targeted based on desired criteria (col.16, lines 1-7). Hertz suggests querying and database matching obviously suggests ability for determining if a privacy preference associated with the requestor has been specified or not and to enable or restrict the ability of an explicitly identified user (col.15, lines 16-20). With Hertz suggesting querying with data mining tools and Moles capable of entering a response in response to a question whether location information is to be transmitted. Thus, suggests the ability to request a privacy preference associated with

the requestor from the user in response to receiving the request if the privacy preference associated with the requestor has not been specified.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Moles with Hertz to teach if a privacy preference associated with the requestor has not been specified, requesting a privacy preference in response to receiving the request because access control dictating profile access and reach ability of the user may be controlled based upon the profile of the requestor such access control may be used to enable/restrict access (Hertz-col.15, lines 11-46 and col.16, lines 1-7).

As per claim 8: See Moles on col.6, lines 57-61 and col.9, lines 51-60; discusses enabling the user to selectively enable and disable location-aware computing includes providing an option during basic input/output system configuration to enable and disable location-aware computing.

As per claim 9: See Moles on col.2, lines 36-39 and col.2, line 66 – col.3, line 2; discusses setting a location privacy setting bit in response to the user selectively enabling or disabling location-aware computing.

As per claim 10: See Moles on col.2, lines 65-67 and Hertz on col.10, lines 24-35; discusses setting the location privacy setting bit includes setting a bit in BIOS memory.

As per claim 11: See Moles on col.2, lines 10-41 and col.6, lines 57-61; discusses receiving, by a computer device, a request for the location property from the requestor, and querying the location privacy setting bit of the computer device, to determine whether location-aware computing is enabled or disabled.

As per claim 12: See Moles on col.9, lines 50-60; discusses setting and querying are performed using Advanced Configuration and Power Interface (ACPI)-based techniques.

As per claim 13:

Moles disclose a machine-accessible medium storing instructions that, when executed by a machine, cause the machine to:

in response to receiving a request from a requestor for a location, determine whether a privacy preferences associated with the requestor have been specified; and **(col.2, lines 10-15 and col.6, lines 21-25)**

if a privacy preference associated with the requestor have been specified **(col.7, lines 5-12 and col.10, lines 37-57)**, applying each privacy preference to determine whether to provide a location property or withhold the location property; and **(col.6, lines 10-20 and col.7, lines 10-13)**

if a privacy preference associated with the requestor have not been specified **(col.2, line 60-col.3, line 2 col.9, lines 50-53)**, request **(col.6, line 20-col.7, line 3)** that the privacy preference associated with each of the plurality of location properties **(col.9, lines 50-60 and col.11, lines 15-18)** for the requester from the user, wherein the privacy preferences indicates location information to be shared with and/or blocked from the requestor. **(col.6, line 56 – col.7, line 28 and col.8, lines 37-64)**

The computer device can broadly be given as a wireless mobile station (col.4, lines 45-54). Moles teach the operator or (authorized) party requesting or receiving the mobile station's location reads on the requestor for the location of the computer device

(col.2, lines 20-22 and 38-40). Moles discloses the user have the ability to selectively

transmit the location of the wireless mobile station to authorized parties (col.2, lines 38-

40). Moles also disclose a method fro selectively disabling the transmission of

information concerning the location of the wireless mobile station (col.3, lines 40-44).

This obviously suggests the ability to set to transmit or not transmit the location property

to a particular requestor(s) which in Moles' instance, is for authorized parties (col.8,

lines 37-64). Thus, Moles suggests the claimed determining whether a privacy

preference associated with the requestor has been specified.

The claimed location properties can broadly be interpreted as data or information

relating to the location which as claimed is associated to the computing device. Hence,

the location properties can be reasonably be given as geographic location in terms of

latitude and longitude of the mobile station (col.6, lines 10-20 and col.7, lines 10-13).

Moles discusses the claimed privacy preference as the privacy flag where a value that

has been set determines whether information of the location of the mobile station is to

be transmitted (col.2, line 60 – col.3, line 2 and col.6, lines 56-61).

In addition, Moles discloses the privacy flag can selectively set to cause wireless the

mobile station to not transmit location information of the mobile station and can set a

value of location privacy flag whether location information is to be transmitted (col.6, line

56-col.7, line 5). Thus, obviously suggested sending location information if the privacy

preference associated with the requestor has not been specified otherwise. However,

Moles did not clearly explain the claimed requesting a privacy preference associated

with the requestor if a privacy preference associated with the requestor has not been
specified.

Hertz, et al. teaches the location enhanced information delivery system can
improve the user-user automatic matching techniques by notifying users of other users
that are located in or near the same vicinity and match the profile conditions as
consistent with the privacy policies of users (col.13, lines 30-42). Hertz discloses
access control criteria dictating profile access and reach ability of the user may be
controlled accordingly based upon the profile of the requestor and/or the nature of the
request (col.15, lines 11-36). Hertz includes the ability of queries and tasks
requirements in the form of request (col.15, lines 4-6). Access control criteria dictating
profile access and reach ability of the user and construction of conveniently navigable
hierarchical menus (col.14, lines 15-17 and col.15, lines 12-25). Hertz also discloses
data mining tools can be used to enable advertisers to identify relevant features and
may enter rules that specify how users are to be targeted based on desired criteria
(col.16, lines 1-7). Hertz suggests querying and database matching obviously suggests
ability for determining if a privacy preference associated with the requestor has been
specified or not and to enable or restrict the ability of an explicitly identified user (col.15,
lines 16-20). With Hertz suggesting querying with data mining tools and Moles capable
of entering a response in response to a question whether location information is to be
transmitted. Thus, suggests the ability to request a privacy preference associated with
the requestor from the user in response to receiving the request if the privacy
preference associated with the requestor has not been specified.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Moles with Hertz to teach if a privacy preference associated with the requestor has not been specified, requesting a privacy preference in response to receiving the request because access control dictating profile access and reach ability of the user may be controlled based upon the profile of the requestor such access control may be used to enable/restrict access (Hertz-col.15, lines 11-46 and col.16, lines 1-7).

As per claim 14: Cancelled

As per claim 15: See Moles on col.6, lines 21-24 and Hertz on col.18, lines 52-55; discloses provide a pop-up dialog box to request the privacy preference.

As per claim 16: See Moles on col.2, line 66 – col.3, line 2; discloses determine whether the machine is enabled for location-aware computing.

As per claim 17: See Moles on col.7, lines 14-45 and Hertz on col.13, lines 24-46 and col.15, lines 3-45; discloses if the machine is not enabled for location-aware computing, preventing the machine from providing the requested location property regardless of whether the privacy preference has been specified and, if specified, regardless of the contents of the privacy preference.

As per claim 18:

Moles disclose a method comprising:

in response to receiving a request for a location from a requestor, determining whether a computing device is enabled for location-aware computing; **(col.2, lines 10-40 and col.6, lines 21-25)**

if the computing device is enabled for location-aware computing **(col.2, line 60 –
col.3, line 2)**, determining whether a privacy preferences associated with a plurality of
location properties for the requestor have been specified; **(col.7, lines 10-13)**

if the privacy preference associated with each of the plurality of location
properties for the requestor have been specified **(col.9, lines 50-60 and col.11, lines 15-
18)**, applying each privacy preference to determine whether to provide the location
property or withhold the location property; and **(col.7, lines 5-12 and col.10, lines 37-57)**

if the privacy preferences associated with each of the plurality of location
properties for the requestor have not been specified **(col.2, line 60-col.3, line 2 col.9,
lines 50-53)**, requesting the privacy preferences **(col.6, line 20-col.7, line 3)** associated
with each of the plurality of location properties for the requestor, wherein the privacy
preferences indicates location information is to be shared with and/or blocked from the
requestor. **(col.6, line 56 – col.7, line 28 and col.8, lines 37-64)**

The computer device can broadly be given as a wireless mobile station (col.4,
lines 45-54). Moles teach the operator or (authorized) party requesting or receiving the
mobile station's location reads on the requestor for the location of the computer device
(col.2, lines 20-22 and 38-40). Moles discloses the user have the ability to selectively
transmit the location of the wireless mobile station to authorized parties (col.2, lines 38-
40). Moles also disclose a method fro selectively disabling the transmission of
information concerning the location of the wireless mobile station (col.3, lines 40-44).
This obviously suggests the ability to set to transmit or not transmit the location property
to a particular requestor(s) which in Moles' instance, is for authorized parties (col.8,

lines 37-64). Thus, Moles suggests the claimed determining whether a privacy preference associated with the requestor has been specified.

The claimed location properties can broadly be interpreted as data or information relating to the location which as claimed is associated to the computing device. Hence, the location properties can be reasonably be given as geographic location in terms of latitude and longitude of the mobile station (col.6, lines 10-20 and col.7, lines 10-13). Moles discusses the claimed privacy preference as the privacy flag where a value that has been set determines whether information of the location of the mobile station is to be transmitted (col.2, line 60 – col.3, line 2 and col.6, lines 56-61).

In addition, Moles discloses the privacy flag can selectively set to cause wireless the mobile station to not transmit location information of the mobile station and can set a value of location privacy flag whether location information is to be transmitted (col.6, line 56-col.7, line 5). Thus, obviously suggested sending location information if the privacy preference associated with the requestor has not been specified otherwise. However, Moles did not clearly explain the claimed requesting a privacy preference associated with the requestor if a privacy preference associated with the requestor has not been specified.

Hertz, et al. teaches the location enhanced information delivery system can improve the user-user automatic matching techniques by notifying users of other users that are located in or near the same vicinity and match the profile conditions as consistent with the privacy policies of users (col.13, lines 30-42). Hertz discloses access control criteria dictating profile access and reach ability of the user may be

controlled accordingly based upon the profile of the requestor and/or the nature of the request (col.15, lines 11-36). Hertz includes the ability of queries and tasks requirements in the form of request (col.15, lines 4-6). Access control criteria dictating profile access and reach ability of the user and construction of conveniently navigable hierarchical menus (col.14, lines 15-17 and col.15, lines 12-25). Hertz also discloses data mining tools can be used to enable advertisers to identify relevant features and may enter rules that specify how users are to be targeted based on desired criteria (col.16, lines 1-7). Hertz suggests querying and database matching obviously suggests ability for determining if a privacy preference associated with the requestor has been specified or not and to enable or restrict the ability of an explicitly identified user (col.15, lines 16-20). With Hertz suggesting querying with data mining tools and Moles capable of entering a response in response to a question whether location information is to be transmitted. Thus, suggests the ability to request a privacy preference associated with the requestor from the user in response to receiving the request if the privacy preference associated with the requestor has not been specified.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Moles with Hertz to teach if a privacy preference associated with the requestor has not been specified, requesting a privacy preference in response to receiving the request because access control dictating profile access and reach ability of the user may be controlled based upon the profile of the requestor such access control may be used to enable/restrict access (Hertz-col.15, lines 11-46 and col.16, lines 1-7).

As per claim 19: See Moles on col.6, lines 21-24 and Hertz on col.18, lines 52-55;

discloses requesting the privacy preference comprises providing a pop-up dialog box.

As per claim 20: See Moles on col.2, lines 65-67 and Hertz on col.10, lines 24-35;

discloses determining whether a computing device is enabled for location-aware

computing comprises determining a value stored in a location privacy setting in basic

input/output system (BIOS) memory.

As per claim 21: See Moles on col.6, lines 56-57; discloses enabling a user to enable

and disable location-aware computing through a BIOS configuration routine.

As per claim 22: See Moles on col.9, lines 9-34 and 50-60; discloses using WMI/ACPI

instrumentation techniques to set and determine the value stored in the location privacy

setting.

As per claim 23:

Moles disclose a system comprising:

a bus to communicate information; **(col.5, lines 21-22)**

a processor coupled to the bus; **(col.4, lines 51-57)**

a memory coupled to the bus to store information; **(col.2, lines 65-66)**

an antenna coupled to the bus to receive a signal to indicate a location of

the system; and **(col.2, lines 5-15)**

a machine-accessible storage medium storing instructions that, when

executed by the processor, cause the system to:

in response to receiving a request for a location associated with the system from

a requestor **(col.2, lines 10-15 and col.6, lines 21-25)**, determine whether privacy

preferences associated with a plurality of location properties have been specified for the

requestor; and **(col.9, lines 50-60 and col.11, lines 15-18)**

if privacy preferences have been specified, apply each privacy preference to

determine whether to provide or withhold the requested location property;   **(col.7, lines**

5-12 and col.10, lines 37-57)

if privacy preferences associated with the plurality of location properties have not

been specified for the requestor **(col.2, line 60-col.3, line 2 col.9, lines 50-53)**, request

that the privacy preferences be specified, wherein the privacy preferences indicate

location information to be shared with and/or blocked from the requestor. **(col.6, line 56 –**

col.7, line 28 and col.8, lines 37-64)

The computer device can broadly be given as a wireless mobile station (col.4,

lines 45-54). Moles teach the operator or (authorized) party requesting or receiving the

mobile station's location reads on the requestor for the location of the computer device

(col.2, lines 20-22 and 38-40). Moles discloses the user have the ability to selectively

transmit the location of the wireless mobile station to authorized parties (col.2, lines 38-

40). Moles also disclose a method fro selectively disabling the transmission of

information concerning the location of the wireless mobile station (col.3, lines 40-44).

This obviously suggests the ability to set to transmit or not transmit the location property

to a particular requestor(s) which in Moles' instance, is for authorized parties (col.8,

lines 37-64). Thus, Moles suggests the claimed determining whether a privacy

preference associated with the requestor has been specified.

The claimed location properties can broadly be interpreted as data or information relating to the location which as claimed is associated to the computing device. Hence, the location properties can be reasonably be given as geographic location in terms of latitude and longitude of the mobile station (col.6, lines 10-20 and col.7, lines 10-13). Moles discusses the claimed privacy preference as the privacy flag where a value that has been set determines whether information of the location of the mobile station is to be transmitted (col.2, line 60 – col.3, line 2 and col.6, lines 56-61).

In addition, Moles discloses the privacy flag can selectively set to cause wireless the mobile station to not transmit location information of the mobile station and can set a value of location privacy flag whether location information is to be transmitted (col.6, line 56-col.7, line 5). Thus, obviously suggested sending location information if the privacy preference associated with the requestor has not been specified otherwise. However, Moles did not clearly explain the claimed requesting a privacy preference associated with the requestor if a privacy preference associated with the requestor has not been specified.

Hertz, et al. teaches the location enhanced information delivery system can improve the user-user automatic matching techniques by notifying users of other users that are located in or near the same vicinity and match the profile conditions as consistent with the privacy policies of users (col.13, lines 30-42). Hertz discloses access control criteria dictating profile access and reach ability of the user may be controlled accordingly based upon the profile of the requestor and/or the nature of the request (col.15, lines 11-36). Hertz includes the ability of queries and tasks

requirements in the form of request (col.15, lines 4-6). Access control criteria dictating profile access and reach ability of the user and construction of conveniently navigable hierarchical menus (col.14, lines 15-17 and col.15, lines 12-25). Hertz also discloses data mining tools can be used to enable advertisers to identify relevant features and may enter rules that specify how users are to be targeted based on desired criteria (col.16, lines 1-7). Hertz suggests querying and database matching obviously suggests ability for determining if a privacy preference associated with the requestor has been specified or not and to enable or restrict the ability of an explicitly identified user (col.15, lines 16-20). With Hertz suggesting querying with data mining tools and Moles capable of entering a response in response to a question whether location information is to be transmitted. Thus, suggests the ability to request a privacy preference associated with the requestor from the user in response to receiving the request if the privacy preference associated with the requestor has not been specified.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Moles with Hertz to teach if a privacy preference associated with the requestor has not been specified, requesting a privacy preference in response to receiving the request because access control dictating profile access and reach ability of the user may be controlled based upon the profile of the requestor such access control may be used to enable/restrict access (Hertz-col.15, lines 11-46 and col.16, lines 1-7).

As per claim 24: See Moles on col.2, line 66 – col.3, line 2; discloses the machine-accessible storage medium further stores instructions that, when executed by the

processor, cause the system to determine whether the system is enabled for location-aware computing.

As per claim 25: See Moles on col.2, lines 65-67 and Hertz on col.10, lines 24-35; discloses the memory includes a basic input/output system (BIOS) memory and wherein determining whether the system is enabled for location-aware computing includes determining a value stored in a location in the BIOS memory.

As per claim 26: Cancelled

As per claim 27: See Moles on col.6, lines 21-24 and Hertz on col.18, lines 52-55; discloses requesting the privacy preference includes providing a pop-up dialog box.

As per claim 28: See Moles on col.4, lines 45-65; discloses the requestor is one of a client application or a location-based service.

As per claim 29:

Moles disclose a computer-implemented method comprising:

receiving, by a computer device, a query requesting one or more location properties; **(col.2, lines 10-15 and col.6, lines 8-25)**

determining if location aware computing is enabled for the computer device; **(col.6, lines 56-60)**

if the location aware computing is enabled, then determining whether user privacy preferences have been specified; **(col.2, line 60 – col.3, line 2;** *privacy flag***)**

if user privacy preferences have not been specified **(col.2, line 60-col.3, line 2 col.9, lines 50-53)**, requesting user privacy preferences **(col.6, line 20-24 and col.6, line**

56-col.7, line 3) associated with each of the one or more location properties requested **(col.9, lines 50-60 and col.11, lines 15-18)**, wherein the privacy preference indicates location information is to be shared with and/or blocked from the requestor; **(col.7, lines 6-28 and col.8, lines 37-64)**

determining whether privacy is indicated for each of the requested one or more location properties; **(col.9, line 50 - col.10, line 5)**

for any of the requested one or more location properties in which privacy is not indicated, obtaining the requested one or more location properties and sending the requested one or more location properties; and **(col.7, lines 14-18 and col.9, lines 50-53)**

for any of the requested one or more location properties in which privacy is indicated, blocking the requested one or more location properties for which privacy is indicated. **(col.6, line 56 – col.7, line 28 and col.8, lines 37-64)**

The computer device can broadly be given as a wireless mobile station (col.4, lines 45-54). Moles teach the operator or (authorized) party requesting or receiving the mobile station's location reads on the requestor for the location of the computer device (col.2, lines 20-22 and 38-40). Moles discloses the user have the ability to selectively transmit the location of the wireless mobile station to authorized parties (col.2, lines 38-40). Moles also disclose a method fro selectively disabling the transmission of information concerning the location of the wireless mobile station (col.3, lines 40-44). This obviously suggests the ability to set to transmit or not transmit the location property

to a particular requestor(s) which in Moles' instance, is for authorized parties (col.8, lines 37-64). Thus, Moles suggests the claimed determining whether a privacy preference associated with the requestor has been specified.

The claimed location properties can broadly be interpreted as data or information relating to the location which as claimed is associated to the computing device. Hence, the location properties can be reasonably be given as geographic location in terms of latitude and longitude of the mobile station (col.6, lines 10-20 and col.7, lines 10-13). Moles discusses the claimed privacy preference as the privacy flag where a value that has been set determines whether information of the location of the mobile station is to be transmitted (col.2, line 60 – col.3, line 2 and col.6, lines 56-61).

In addition, Moles discloses the privacy flag can selectively set to cause wireless the mobile station to not transmit location information of the mobile station and can set a value of location privacy flag whether location information is to be transmitted (col.6, line 56-col.7, line 5). Thus, obviously suggested sending location information if the privacy preference associated with the requestor has not been specified otherwise. However, Moles did not clearly explain the claimed requesting a privacy preference associated with the requestor if a privacy preference associated with the requestor has not been specified.

Hertz, et al. teaches the location enhanced information delivery system can improve the user-user automatic matching techniques by notifying users of other users that are located in or near the same vicinity and match the profile conditions as consistent with the privacy policies of users (col.13, lines 30-42). Hertz discloses

access control criteria dictating profile access and reach ability of the user may be controlled accordingly based upon the profile of the requestor and/or the nature of the request (col.15, lines 11-36). Hertz includes the ability of queries and tasks requirements in the form of request (col.15, lines 4-6). Access control criteria dictating profile access and reach ability of the user and construction of conveniently navigable hierarchical menus (col.14, lines 15-17 and col.15, lines 12-25). Hertz also discloses data mining tools can be used to enable advertisers to identify relevant features and may enter rules that specify how users are to be targeted based on desired criteria (col.16, lines 1-7). Hertz suggests querying and database matching obviously suggests ability for determining if a privacy preference associated with the requestor has been specified or not and to enable or restrict the ability of an explicitly identified user (col.15, lines 16-20). With Hertz suggesting querying with data mining tools and Moles capable of entering a response in response to a question whether location information is to be transmitted. Thus, suggests the ability to request a privacy preference associated with the requestor from the user in response to receiving the request if the privacy preference associated with the requestor has not been specified.

Therefore, it would have been obvious for a person of ordinary skills in the art to combine the teaching of Moles with Hertz to teach if a privacy preference associated with the requestor has not been specified, requesting a privacy preference in response to receiving the request because access control dictating profile access and reach ability of the user may be controlled based upon the profile of the requestor such access

control may be used to enable/restrict access (Hertz-col.15, lines 11-46 and col.16, lines 1-7).

As per claim 30: See Moles on col.6, lines 21-24 and Hertz on col.18, lines 52-55; discloses the method of claim 29, wherein requesting user privacy preferences associated with each of the one or more location properties includes providing a pop-up dialog box.

As per claim 31: See Moles on col.9, lines 50-53 and col.10, lines 37-57 and Hertz on col.18, lines 52-55; discloses the method of claim 30, wherein providing a pop-up dialog box includes enabling a user to selectively enable and disable privacy preferences for each individual location property.

As per claim 32: See Moles on col.3, lines 30-34 and col.8, lines 37-64 and Hertz on col.15, lines 14-35; discloses the method of claim 1, wherein a privacy menu allows the user to select the privacy preference for the requestor.

As per claim 33: See Moles on col.6, lines 8-20 and col.7, lines 6-28; discloses the method of claim 32, wherein a privacy menu comprises location properties, the location properties including at least one of latitude, longitude, altitude, street address, city, state, postal code, and/or country, and wherein the user may select one, more than one, or none of the location properties for the privacy preference of the requestor.

Conclusion

5.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Leynna T. Truvan whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM) and telework on Wednesday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent
Application Information Retrieval (PAIR) system. Status information for published applications
may be obtained from either Private PAIR or Public PAIR. Status information for unpublished
applications is available through Private PAIR only. For more information about the PAIR
system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private
PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you
would like assistance from a USPTO Customer Service Representative or access to the
automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/L. T. T./
Examiner, Art Unit 2435

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435